McAfee Labs Security Advisory

McAfee
Together is power.

EXECUTIVE SUMMARY

June 12, 2018 | MTIS18-016

Since the last McAfee® Labs Security Advisory (May 8), the following noteworthy event has taken place:

- Patches are available for multiple Microsoft security vulnerabilities

NEW THREAT OVERVIEW

(MSPT-Jun2018) Microsoft Windows PowerShell Security Bypass (CVE-2018-8221)

MTIS18-016-A

IMPORTANCE:	High
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Windows Kernel Privilege Escalation (CVE-2018-8224)

MTIS18-016-B

IMPORTANCE:	High
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Windows DNSAPI Remote Code Execution (CVE-2018-8225)

MTIS18-016-C

IMPORTANCE:	High
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Windows HTTP 2.0 Denial of Service (CVE-2018-8226)

MTIS18-016-D

IMPORTANCE:	High
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Edge Chakra Scripting Engine Remote Code Execution Vulnerability (CVE-2018-8227)

MTIS18-016-E

IMPORTANCE:	High
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Edge Chakra Scripting Engine Remote Code Execution Vulnerability (CVE-2018-8229)

MTIS18-016-F

IMPORTANCE:	High
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Windows HTTP Protocol Stack Remote Code Execution (CVE-2018-8231)

MTIS18-016-G

IMPORTANCE:	High
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Windows Win32k Privilege Escalation (CVE-2018-8233)

MTIS18-016-H

IMPORTANCE:	High
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Edge Memory Handler Information Disclosure Vulnerability (CVE-2018-8234)

MTIS18-016-I

IMPORTANCE:	High
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Edge Security Feature Bypass Vulnerability (CVE-2018-8235)

MTIS18-016-J

IMPORTANCE:	High
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Edge Improperly Accesses Objects Remote Code Execution Vulnerability (CVE-2018-8236)

MTIS18-016-K

IMPORTANCE:	High
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Windows GDI Information Disclosure (CVE-2018-8239)

MTIS18-016-L

IMPORTANCE:	High
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Outlook Attachment Headers Privilege Escalation (CVE-2018-8244)
MTIS18-016-M

IMPORTANCE: High
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Publisher OLE Objects Privilege Escalation (CVE-2018-8245)
MTIS18-016-N

IMPORTANCE: High
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Excel Memory Information Disclosure (CVE-2018-8246)
MTIS18-016-O

IMPORTANCE: High
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Office Handle Web Requests Privilege Escalation (CVE-2018-8247)
MTIS18-016-P

IMPORTANCE: High
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Excel Remote Code Execution (CVE-2018-8248)
MTIS18-016-Q

IMPORTANCE: High
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Internet Explorer Memory Remote Code Execution (CVE-2018-8249)
MTIS18-016-R

IMPORTANCE: High
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Windows Media Foundation Memory Remote Code Execution (CVE-2018-8251)
MTIS18-016-S

IMPORTANCE: High
COVERED PRODUCTS: Vulnerability Manager
UNDER ANALYSIS: Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Sharepoint Web Request Sanitization Privilege Escalation (CVE-2018-8252)
MTIS18-016-T

IMPORTANCE: High
COVERED PRODUCTS: Vulnerability Manager

UNDER ANALYSIS:	Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Sharepoint Web Request Sanitization Privilege Escalation (CVE-2018-8254)

MTIS18-016-U

IMPORTANCE:	High
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Chakra Scripting Engine Remote Code Execution (CVE-2018-8243)

MTIS18-016-V

IMPORTANCE:	High
COVERED PRODUCTS:	
UNDER ANALYSIS:	Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Internet Explorer Handles Objects in Memory Remote Code Execution (CVE-2018-8267)

MTIS18-016-W

IMPORTANCE:	High
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	Firewall Enterprise

Back to top

(MSPT-Jun2018) Microsoft Windows Desktop Bridge Privilege Escalation Vulnerability (CVE-2018-8214)

MTIS18-016-X

IMPORTANCE:	High
COVERED PRODUCTS:	Vulnerability Manager
UNDER ANALYSIS:	

Back to top

THREAT DETAILS

(MSPT-Jun2018) Microsoft Windows PowerShell Security Bypass (CVE-2018-8221)

MTIS18-016-A

THREAT IDENTIFIER(S)	CVE-2018-8221
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to security bypass. The flaw lies in the PowerShell component. Successful exploitation by a remote attacker could result in the bypass of intended access restrictions. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.

POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Windows Kernel Privilege Escalation (CVE-2018-8224)

MTIS18-016-B

THREAT IDENTIFIER(S)	CVE-2018-8224
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Kernel. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Windows DNSAPI Remote Code Execution (CVE-2018-8225)

MTIS18-016-C

THREAT IDENTIFIER(S)	CVE-2018-8225
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Critical
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in DNSAPI.dll. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.

VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Windows HTTP 2.0 Denial of Service (CVE-2018-8226)

MTIS18-016-D

THREAT IDENTIFIER(S)	CVE-2018-8226
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to a denial of service. The flaw lies in the HTTP 2.0 component. Successful exploitation by a remote attacker could result in a denial of service condition.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Edge Chakra Scripting Engine Remote Code Execution Vulnerability (CVE-2018-8227)

MTIS18-016-E

THREAT IDENTIFIER(S)	CVE-2018-8227
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	Yes

DESCRIPTION	A vulnerability in some versions of Microsoft Edge could lead to remote code execution. The flaw lies in the Chakra Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Edge Chakra Scripting Engine Remote Code Execution Vulnerability (CVE-2018-8229)

MTIS18-016-F

THREAT IDENTIFIER(S)	CVE-2018-8229
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Edge could lead to remote code execution. The flaw lies in the Chakra Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Windows HTTP Protocol Stack Remote Code Execution (CVE-2018-8231)

MTIS18-016-G

THREAT IDENTIFIER(S)	CVE-2018-8231
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in the Win32k component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Windows Win32k Privilege Escalation (CVE-2018-8233)

MTIS18-016-H

THREAT IDENTIFIER(S)	CVE-2018-8233
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Edge could lead to privilege escalation. The flaw lies in the Memory Handler component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.

APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Edge Memory Handler Information Disclosure Vulnerability (CVE-2018-8234)

MTIS18-016-I

THREAT IDENTIFIER(S)	CVE-2018-8234
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Edge could lead to information disclosure. The flaw lies in the Memory Handler component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Edge Security Feature Bypass Vulnerability (CVE-2018-8235)

MTIS18-016-J

THREAT IDENTIFIER(S)	CVE-2018-8235
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Edge could lead to security bypass. The flaw lies in the Improperly Accesses Objects component. Successful exploitation by a remote attacker could result in security bypass. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.

VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Edge Improperly Accesses Objects Remote Code Execution Vulnerability (CVE-2018-8236)

MTIS18-016-K

THREAT IDENTIFIER(S)	CVE-2018-8236
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in the improperly accessesd objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Windows GDI Information Disclosure (CVE-2018-8239)

MTIS18-016-L

THREAT IDENTIFIER(S)	CVE-2018-8239
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
	A vulnerability in some versions of Microsoft Outlook could lead to information disclosure. The flaw lies in the Attachment Headers component. Successful

DESCRIPTION	exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Outlook Attachment Headers Privilege Escalation (CVE-2018-8244)

MTIS18-016-M

THREAT IDENTIFIER(S)	CVE-2018-8244
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Outlook could lead to privilege escalation. The flaw is due to improper handling of attachment headers. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Publisher OLE Objects Privilege Escalation (CVE-2018-8245)

MTIS18-016-N

THREAT IDENTIFIER(S)	CVE-2018-8245
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Publisher could lead to privilege escalation. The flaw lies in the Memory component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Excel Memory Information Disclosure (CVE-2018-8246)

MTIS18-016-O

THREAT IDENTIFIER(S)	CVE-2018-8246
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Office could lead to information disclosure. The flaw is due to improper handling of objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.

APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Office Handle Web Requests Privilege Escalation (CVE-2018-8247)

MTIS18-016-P

THREAT IDENTIFIER(S)	CVE-2018-8247
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Excel could lead to privilege escalation. The flaw lies in the Handle Objects Memory component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Excel Remote Code Execution (CVE-2018-8248)

MTIS18-016-Q

THREAT IDENTIFIER(S)	CVE-2018-8248
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Excel could lead to remote code execution. The flaw is due to improper handling of objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.

VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Internet Explorer Memory Remote Code Execution (CVE-2018-8249)

MTIS18-016-R

THREAT IDENTIFIER(S)	CVE-2018-8249
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution. The flaw lies in a memory access error. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Windows Media Foundation Memory Remote Code Execution (CVE-2018-8251)

MTIS18-016-S

THREAT IDENTIFIER(S)	CVE-2018-8251
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Sharepoint could lead to remote code execution. The flaw lies in the Web Request Sanitization component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The

	exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Sharepoint Web Request Sanitization Privilege Escalation (CVE-2018-8252)

MTIS18-016-T

THREAT IDENTIFIER(S)	CVE-2018-8252
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft Sharepoint could lead to privilege escalation. The flaw lies in the Web Request Sanitization component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Sharepoint Web Request Sanitization Privilege Escalation (CVE-2018-8254)

MTIS18-016-U

THREAT IDENTIFIER(S)	CVE-2018-8254
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft could lead to privilege escalation. The flaw lies in the component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Chakra Scripting Engine Remote Code Execution (CVE-2018-8243)

MTIS18-016-V

THREAT IDENTIFIER(S)	CVE-2018-8243
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Medium
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Chakra Scripting Engine could lead to remote code execution. The flaw lies in a memory handling error. Successful exploitation by a remote attacker could result in the execution of arbitrary code.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	Out of scope.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.

VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Internet Explorer Handles Objects in Memory Remote Code Execution (CVE-2018-8267)

MTIS18-016-W

THREAT IDENTIFIER(S)	CVE-2018-8267
THREAT TYPE	Vulnerability
RISK ASSESSMENT	High
MAIN THREAT VECTORS	Web
USER INTERACTION REQUIRED	Yes
DESCRIPTION	A vulnerability in some versions of Microsoft could lead to remote code execution. The flaw lies in the scripting engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	Coverage not warranted.
VIRUS SCAN ENTERPRISE SCAN BOP	Out of scope.
HOST IPS	Out of scope.
NETWORK SECURITY PLATFORM	Coverage not warranted.
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.
WEB GATEWAY	Coverage not warranted.
REMEDIATION MANAGER	Not applicable.
POLICY AUDITOR	An upcoming SCAP content release will contain coverage for this issue.
NETWORK ACCESS CONTROL	An upcoming SCAP content release will contain coverage for this issue.
FIREWALL ENTERPRISE	Under analysis.
APPLICATION CONTROL	Out of scope.
DATABASE ACTIVITY MONITORING	Out of scope.
VULNERABILITY MANAGER FOR DATABASES	Out of scope.
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

(MSPT-Jun2018) Microsoft Windows Desktop Bridge Privilege Escalation Vulnerability (CVE-2018-8214)

MTIS18-016-X

THREAT IDENTIFIER(S)	CVE-2018-8214
THREAT TYPE	Vulnerability
RISK ASSESSMENT	Low
MAIN THREAT VECTORS	Locally logged-on user
USER INTERACTION REQUIRED	No
DESCRIPTION	A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Desktop Bridge component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.
IMPORTANCE	High. On June 12, Microsoft released an update to address this vulnerability
MCAFEE PRODUCT COVERAGE	
DAT FILES	No Coverage Status
VIRUS SCAN ENTERPRISE SCAN BOP	No Coverage Status
HOST IPS	No Coverage Status
NETWORK SECURITY PLATFORM	No Coverage Status
VULNERABILITY MANAGER	The FSL/MVM package of June 12 includes a vulnerability check to assess if your systems are at risk.

WEB GATEWAY	No Coverage Status
REMEDIATION MANAGER	No Coverage Status
POLICY AUDITOR	No Coverage Status
NETWORK ACCESS CONTROL	No Coverage Status
FIREWALL ENTERPRISE	No Coverage Status
APPLICATION CONTROL	No Coverage Status
DATABASE ACTIVITY MONITORING	No Coverage Status
VULNERABILITY MANAGER FOR DATABASES	No Coverage Status
ADDITIONAL INFORMATION	Microsoft: Security Update Summary

Back to top

For McAfee Technical Support, click here.

For Multi-National Phone Support, click here.

McAfee values your feedback on this Security Advisory. Please reply to this mail with your comments.

*The information provided is only for the use and convenience of McAfee's customers in connection with their McAfee products, and applies only to the threats described herein. McAfee product coverage statements are limited to known attack vectors and should not be considered comprehensive. THE INFORMATION PROVIDED HEREIN IS PROVIDED "AS IS" AND IS SUBJECT TO CHANGE WITHOUT NOTICE.

McAfee, Inc. 2821 Mission College Blvd, Santa Clara, CA 95054 888.847.8766 www.mcafee.com